MASON HAYES & CURRAN

TECHNOLOGY INSIGHT | SEPTEMBER 2025

NIS2 Considerations for the Life Sciences Sector

Key changes and practical steps to ensure compliance

Cyber security is critical to every aspect of a Life Sciences business. It safeguards sensitive data and systems, and is essential for maintaining regulatory compliance and stakeholder trust. Emerging laws and legislative reform make compliance a moving target.

In this article, we:

1. Highlight the key provisions of the NIS2 Directive
2. Examine its application to the Life Sciences sector, and
3. Outline the practical steps organisations should take to ensure compliance.

What is NIS2?

NIS2 forms part of a package of measures to improve the cyber security and resilience of critical public and private sector organisations. NIS2 will require an overhaul of how organisations approach cyber security and puts leadership accountability at its core. NIS2 is currently being transposed into the national law of each EU Member State, meaning the exact application of the rules will vary from country to country. As a result, this will create a compliance challenge for multinational organisations.

Application to the Life Sciences sector

In basic terms, subject to meeting certain size criteria, NIS2 will apply to entities in sectors which are considered critical to the EU's security and the functioning of its economy. These include the health, food and manufacturing sectors. In particular, for Life Sciences companies, again subject to meeting certain size criteria, NIS2 will apply to the following activities:

- Healthcare providers
- EU reference labs
- R&D of medicinal products
- Manufacturing basic pharmaceutical products / preparations
- Manufacturing medical devices and in vitro diagnostic medical devices
- Manufacturing medical devices considered to be critical during a public health emergency
- Manufacturing, production and distribution of chemicals
- Manufacturing of electronic products
- Food business

Generally, organisations in the Life Sciences sector will be subject to the separate and concurrent jurisdiction of each Member State in which they are established. These various national rules are causing significant headaches for multinational organisations, as the rules can vary significantly from Member State to Member State. For example, in some countries, the definition of the health sector has been expanded to include the distribution and importation of medical products, while in other jurisdictions these sectors are out of scope.

The rules mean that multinational organisations must comply with all local laws transposing NIS2 in every Member State where they are established. They must also register with the relevant competent authority in each Member State. In addition, they are required to report significant cross-border cyber security incidents to the relevant competent authorities. Senior management of organisations in each Member State are responsible for compliance. The stakes are high, as boards and senior management can be held directly accountable for compliance failings. This is causing particular issues for multinational Life Sciences organisations. Traditionally, cyber security is the responsibility of the head office or parent company, with affiliates simply relying on the measures adopted by the parent organisation.

Key issues for Life Sciences businesses

- **Registration:** In-scope entities will need to register with their national competent authority in each Member State in which they are established. Member States have each imposed different registration deadlines and procedures for registering, which can be complex.
- **Risk Management Measures:** Under NIS2, each Member State will establish a set of risk management measures (RMMs) that organisations will be required to implement, as appropriate. The management body of each organisation, such as the board of directors, must approve the RMMs of their own organisation. They must also oversee the implementation of the RMMs. In certain jurisdictions, members of the management body risk being held personally liable for any infringements. The RMMs vary across each Member State, with different assessment and certification frameworks being introduced. These circumstances will inevitably lead to inconsistent approaches across the EU. For example, there is a requirement in Hungary and Romania to appoint a specified local auditor to assess compliance. However, this requirement doesn't exist in other Member States at present.
- **Supply chain due diligence:** As part of their risk management measures, NIS2 requires entities to carry out due diligence of their supply chain security. Organisations will have to ensure that they have confidence in the network and information systems of their suppliers, in addition to their own network and information systems.
- **Incident reporting:** In-scope Life Sciences organisations will be obliged to report significant cyber security incidents to the relevant competent authority. An initial report must be made within 24 hours of the organisation becoming aware of the incident. Follow up reports must be made within 72 hours, with the final report to be made in 30 days. Each country will have different reporting mechanisms and reporting requirements. As a result, handling a cross-border incident will be challenging. Multinational organisations should ensure that they have internal reporting procedures in place so if a cross-border incident occur, there is an established process to follow. These procedures should be tested through the use of tabletop exercises.
- **Training:** Training must also be provided to management bodies to equip them to meet their obligations to approve and implement RMMs. Cyber security training should also be provided to all staff.

> “*NIS2 makes cyber security a board-level responsibility for Life Sciences firms, with cross-border compliance, supplier checks, and rapid incident reporting now non-negotiable.*

KEY DATES

EU Member States are each at different stages in their transposition of the NIS2 Directive into national law.

NIS2 is expected to come into effect in Ireland by the end of 2025 or early 2026. We recommend that Life Sciences organisations based in Ireland begin their preparations for the coming into force of NIS2 sooner than later.

NIS2 is expected to come into effect in Ireland by the end of 2025 or early 2026. We recommend that Life Sciences organisations based in Ireland begin their preparations for the coming into force of NIS2 sooner than later.

10 Practical steps **for compliance**

01 Identify the Member State(s) where your organisation is established.

02 Assess whether your entity falls within the scope of NIS2 in each of those Member States, taking account of the local law transposing NIS2.

03 Register with the relevant competent authority in each Member State where the organisation is established, keeping in mind the deadlines for registration varies across countries.

04 Identify key variations in approaches across jurisdictions where your organisation is subject to NIS2. Align risk management measures accordingly.

05 Work with teams on the ground in each of your locations to assess your existing cyber security infrastructure. Also, run risk assessments identifying any weaknesses in your network or your processes.

06 Consider whether you will adopt any certifications such as ISO 27001.

07 Identify your direct suppliers and carry out due diligence of their cyber security practices.

08 Develop your incident reporting plans which set out the flow of how your organisation will respond to and report a significant incident. Test these plans through tabletop exercises.

09 Ensure that you have plans in place for business continuity in case of a significant incident including back up management, disaster recovery and crisis management.

10 Develop a single approach for the management body. Also, deploy and staff training that works across Member States.

MASON HAYES & CURRAN

Dublin London New York San Francisco

ABOUT US

Cyber security law is a rapidly evolving area. Emerging laws and legislative reform make compliance a moving target. Our team understands and foresees the challenges which clients come up against in this area. We have the knowledge and skills to overcome the most complex of problems.

Our Cyber Security team provides advice across the entire suite of cyber security laws including:

- NIS2
- GDPR
- The Cyber Resilience Act
- The ePrivacy Directive, and
- The Telecoms Framework.

Our team supports clients on both domestic and pan European compliance programmes across these emerging legal frameworks. As members of Cyber Ireland, we are at the fore of this rapidly evolving ecosystem.

As a founding member of the European Cyber Law Network, which constitutes lawyers across the EU and the UK, our Cyber Security team can co-ordinate and provide support on pan European compliance and cross-border incidents.

We also work with clients on all issues around national and cross-border security incidents and personal data breaches at each stage of the journey - from Data Breach Readiness to Incident Response Management.

When a cyber incident or personal data breach occurs, a timely legal and strategic response is crucial to mitigate legal risks, limit claims, meet regulatory deadlines and support business continuity and quick recovery. Our Cyber Response team provides a 24/7 one-stop-shop that coordinates technical forensics and ransom negotiations. We also assist clients with regulatory reporting, communication strategies, investigations and post-incident measures to help manage the legal and factual implications of cyber incidents and personal data breaches.

KEY CONTACTS

JULIE AUSTIN
Partner, Data & Technology
jaustin@mhc.ie

MICHAELA HERRON
Partner, Head of Products
mherron@mhc.ie

JAMIE GALLAGHER
Partner, Product Regulatory & Liability
jamesgallagher@mhc.ie

CIARA O'ROURKE
Associate, Data & Technology
corourke@mhc.ie

For more information and expert advice, visit:

MHC.ie/Technology

The contents of this publication are to assist access to information and do not constitute legal or other advice. Readers should obtain their own legal and other advice as may be required.